2011

AUDITORIA INTEGRAL

INSTITUTO REINA DE LOS ANGELES.

Elaborado por:

CORDOBA DIAZ JULIETH KATERINE

MARTI PORTO MARIA ANGELICA

MENDOZA PALECHOR FABIO ENRIQUE

CORPORACIÓN UNIVERSITARIA DE LA COSTA

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

BARRANQUILLA

2011

AUDITORIA INTEGRAL

INSTITUTO REINA DE LOS ANGELES

Elaborado por:

CORDOBA DIAZ JULIETH KATERINE

MARTI PORTO MARIA ANGELICA

MENDOZA PALECHOR FABIO ENRIQUE

CORPORACIÓN UNIVERSITARIA DE LA COSTA

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

BARRANQUILLA

2011

Nota de aceptación

_____
_____
_____
_____

_____
Asesor: Ing. Osvaldo Puello Flórez

Presidente del Jurado

_____
Jurado

_____
Jurado

Barranquilla, 12 de Marzo de 2011

RESUMEN

Instituto Reina De Los Ángeles entidad educativa del sector privado de la ciudad de barranquilla, reconoce las falencias que tiene en sus procesos internos para su manejo organizacional. De allí nace la necesidad de evaluar los diferentes modelos a seguir existentes a nivel local, nacional e internacional y así estar a un nivel superior al manejado por las demás instituciones que trabajan en el mismo sector económico. De esta necesidad surgió nuestro trabajo en donde inicialmente se realizó una charla con la directora de la institución y se hizo un reconocimiento a las instalaciones. Luego el equipo se trazó una meta: detectar las fallas que generen más pérdidas a nivel económico. El instituto Reina de los Ángeles entendió que tener algunos procesos con falencias en su ejecución diaria, se ve representado en la pérdida de imagen de la institución educativa y en la pérdida de ingresos reflejado en sus estados financieros. Por ello nuestro incentivo hacia esta labor es el ayudarles y colaborarles a los dueños de estos procesos al mejoramiento de éstos a través de la generación de las respectivas recomendaciones y la proposición de controles que ayuden a corregir o disminuir la cantidad de riesgos o fallas presentadas en los procesos de la institución.

El modelo utilizado para la evaluación de fallas fue COBIT e ISO 27002 internacionalmente aceptados, los cuales a través de objetivos de control y procesos nos dan una visión más amplia de los fallos que se cometen dentro de la organización dando así un ambiente de transparencia tanto para las personas involucradas y las personas externas a la institución.

La aplicación de los conocimientos obtenidos durante el proceso de formación de la especialización sirvió como base para el buen desarrollo de los pasos empleados y de las recomendaciones dadas a la institución para lograr minimizar las pérdidas generadas por las falencias detectadas.

ABSTRACT

Institute Reina De Los Angeles private educational institution in the city of Barranquilla, have recognized the weaknesses in their internal processes for organizational management itself, there arises the need to assess the different role models that exist at local level national and international, in order to stay ahead of the other institutions that work or maintain the same economic sector. From this need arose where initially our work after making a presentation and recognition of the institute facilities set ourselves a goal, which was to detect faults more losses in the economic and image making or have generated some processes with the deficiencies found, so our incentive to that work was not to harm the institution of our findings, however aiding and abetting by giving the respective recommendations and proposed controls to help correct or reduce the amount of risk or failure at the processes of the institution.

The model used for evaluation or existence of defects in the institution was COBIT and ISO 27000 internationally accepted models who help with the methodology to be aware of the faults committed within the organization thus providing a transparent environment for both people involved and people outside the institution.

The application of knowledge gained during the training process of specialization was the basis for the proper conduct of the steps employed and the recommendations given to the institution in order to minimize the losses generated by the detected failures.

AGRADECIMIENTOS

Gracias a Jehová por permitirme lograr ésta meta más en mi vida, sé que es una de muchas metas que serán inspiradas por él.

Gracias a mis padres por todo su esfuerzo, dedicación y apoyo, por hacer de mí una mujer íntegra y una gran profesional.

Gracias a mis hermanos por tenerme paciencia y apoyarme siempre.

Gracias a los profesores de la especialización por transmitirnos el conocimiento necesario para ser unos excelentes profesionales.

JULIETH CORDOBA DIAZ

AGRADECIMIENTOS

Gracias a Dios por ser mi todo, por ser esa razón que me impulsa a ser mejor, por ser mi gran amigo, mi confidente, mi vida entera.

Gracias a mi madre Griselda Porto Por su cariño, comprensión y apoyo sin condiciones ni medida, por darlo todo por mis hermanos y por mí.

Gracias a mi abuelo Luis Carlos Porto por permitirme llegar hasta este momento tan importante en mi vida y ayudarme a lograr otra meta más en mi carrera.

Gracias a todos los que de una u otra manera me ayudaron a ser lo que soy y a lograr mis metas.

MARIA ANGELICA MARTI PORTO

AGRADECIMIENTOS

Creo que más fuerte que la sabiduría, es la imaginación. Que más potente que la historia, es el mito. Que la esperanza siempre triunfa sobre la experiencia. Que la única cura para el dolor, es la risa, y Que más poderosos que la realidad, son los sueños.

R. Fulghum

Y son los sueños los que nos impulsan hasta el final, por eso:

"Agradezco a DIOS que me permitió la luz para prepararme y cumplir mis objetivos, a mis padres ALVARO y JANETH por su amor, comprensión y paciencia, a mi familia por su apoyo, a mis hermanos por sus ánimos, a mi grupo de trabajo por su apoyo, comprensión".

FABIO MENDOZA PALECHOR

TABLA DE CONTENIDO

TABLA DE IMÁGENES

TABLA DE GRAFICAS

INTRODUCCION

El Instituto Reina de los Ángeles (INRA) es una comunidad educativa de carácter privado en donde se cumplen principios éticos, morales y religiosos que buscan formar individuos integrales y con unos altos niveles académicos preparados para enfrentar el mundo actual.

El INRA en búsqueda del más alto nivel educativo ha querido estar en vanguardia con los más importantes estándares de calidad para respaldar de esta forma la educación brindada a sus estudiantes generando un ambiente competitivo para su vida profesional.

Por este motivo es que fortalecer factores considerados claves para el desempeño de la institución es parte prioritaria de los fundadores de ésta.

La búsqueda de un ambiente adecuado en cuanto a las herramientas y aplicaciones informáticas con las que se cuenta para proteger principalmente la información sensible y confidencial del INRA y además el contar con un ambiente físico óptimo para cada uno de sus alumnos se ha convertido en un constante esfuerzo por implementar mejoras, es por esto que surgió la creación de este proyecto el cual busca satisfacer dichas necesidades a través de la implementación de los antes mencionados estándares internacionales que rigen en el mercado actual, como lo es el ISO 27002 y se tomará como marco de referencia el modelo COBIT, el cual servirá como guía para sustentar todos los cambios que se buscan generar en la institución educativa.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA

Hoy en día implementar o tener como punto de referencia estándares internacionales garantiza buen nivel en el funcionamiento de los procesos para así mantener la diferencia ante las entidades del mismo sector económico y de esta forma lograr una mayor captación de clientes y por consecuente obtener mayores ingresos.

Identificar la necesidad manifestada por el **Instituto Reina de los Ángeles** al reconocer cuáles son sus brechas de seguridad más importantes en cuanto a su información y la administración del ambiente físico de TI, los cuales representan una debilidad en el desarrollo de sus funciones.

Se enfocará esta auditoría hacia los siguientes puntos:

Administración del ambiente físico (DS-12), y Garantizar la seguridad de sistemas (DS5), para esto se hará una observación exhaustiva de las instalaciones y también se realizarán entrevistas al personal de la institución en busca de evidencias que confirmen la información.

Para esta auditoría se tomará como marco de referencia el modelo COBIT y el estándar internacional ISO 27002.

2. JUSTIFICACIÓN E IMPORTANCIA DEL ESTUDIO

2.1 BENEFICIO ORGANIZACIONAL

Este proyecto fue realizado con el fin de brindarle al Instituto Reina de los Ángeles un lineamiento que le permita conocer las mejores prácticas para la correcta administración del ambiente físico de TI y garantizar la seguridad de los sistemas. Todo esto se hará tomando como base el modelo de referencia COBIT, concentrándose principalmente en la aplicación de objetivos de control y en la aplicación del estándar internacional ISO 27002, brindando así una visión mucho más oportuna en cuanto a los riesgos que se pueden estar presentando y que no han sido debidamente administrados.

2.2 BENEFICIO ECONOMICO

Las instituciones colombianas, en especial las del departamento del Atlántico no se han preocupado por la falta de interés o por el desconocimiento de estos.

Estos estándares traen consigo beneficios en cuanto a la mejora de los procesos de esta forma reflejan orden y claridad, trasmitiendo esta imagen a la comunidad, logrando así generar impacto y de esta forma atraer más clientes del mercado, trayendo consigo mayores ingresos económicos.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

- Proporcionar las recomendaciones necesarias para crear un ambiente ideal dentro del Instituto Reina de los Ángeles el cual permitirá brindar lineamientos en cuanto a los niveles de protección de información que deberán ser manejados, creando una mayor cultura en cuanto a la integridad y confidencialidad de ésta, verificar el buen manejo que brindan las aplicaciones que soportan dicha información y crear un ambiente físico de TI conveniente que asegure a todo la plataforma tecnológica contra peligros naturales o fallas humanas.

3.2 OBJETIVOS ESPECIFICOS

- Identificar los riesgos presentes en la infraestructura tecnológica del instituto reina de los ángeles.
- Verificar la seguridad en las aplicaciones (métodos de control acceso).
- Generar lineamientos que permitan soportar y mitigar en gran manera las brechas de seguridad física y de la información que se presentan en la actualidad en el instituto.

4. ALCANCE

A través de un seguimiento integral de los procesos y la verificación del estado de la plataforma tecnológica del instituto reina de los ángeles, se identificaran los puntos más críticos o de mayor impacto, para que estos sean tratarlos con prioridad.

Por ello nuestros puntos clave en el desarrollo de esta auditoría serán:

- Análisis de riesgos.
- Análisis de permisos y roles de los directivos de la institución.
- Verificación de existencia de manuales de usuarios, funciones y técnicos dentro de la institución.

5. MARCOS REFERENCIALES

5.1 MARCO TEORICO

La aceptación de las fallas presentadas en diferentes procesos y en diferentes ambientes ya sea físicos, tecnológicos, se convertirán una oportunidad que llevara de la mano el fortalecer las falencias encontradas, hacer un estudio profundo para lograr controlar vulnerabilidades a través de la aplicación de recomendaciones dirigidas a diversos medios ya sean personas, equipos de auditores, software informáticos entre otros.

Con objeto de ayudar a corregir o controlar las fallas encontradas, nuestro equipo de auditores se propuso enfrentar estas amenazas tomando como referencia los estándares internacionales existentes, Utilizando para ello algunos de sus procesos.

Para el presente trabajo no se presentaron antecedentes de auditorías previas al Instituto Reina de los Ángeles orientadas a la seguridad de la información y la seguridad física del instituto es por esto que nos basaremos en ISO 27002 y en el marco de trabajo de COBIT y específicamente en objetivos de control como son:

- DS 5 Garantizar la seguridad de los sistemas
- DS 12 Administración del ambiente físico

Utilizando los objetivos de control detallado, de los objetivos de control de alto nivel se busca dar solución a las principales preocupaciones que tienen n las directivas.

Basaremos nuestro trabajo principalmente en estos dos objetivos de control (DS 5 Garantizar la seguridad de los sistemas, DS 12 Administración del ambiente físico) para lograr que el colegio cuente con un ambiente físico apropiado para sus equipos de computo previniendo cualquier tipo de amenaza, además buscaremos crear conciencia en cuanto a la necesidad de proteger la

información, logrando que ésta se maneje de acuerdo a los principios de seguridad como lo son la confidencialidad, integridad y disponibilidad.

5.1.1DS 5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS[1]

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad

Control sobre el proceso TI de Garantizar la seguridad de los sistemas que satisface el requisito de negocio de TI para mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad. Enfocándose en la definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad. Se logra con

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular

Se mide con:

- El número de incidentes que dañan la reputación con el público
- El número de sistemas donde no se cumplen los requerimientos de seguridad
- El número de de violaciones en la segregación de tareas.

[1] COBIT. IT GOVERNANCE INSTITUTE. CUARTA EDICION, 2007. Pág. 124

Objetivos de control detallados

DS5.1 Administración de la seguridad de TI Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

DS5.2 Plan de seguridad de TI Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

DS5.3 Administración de identidad Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

DS5.4 Administración de cuentas del usuario Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios

privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad. Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser revisada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

DS5.6 Definición de incidente de seguridad. Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

DS5.7 Protección de la tecnología de seguridad Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

DS5.8 Administración de llaves criptográficas Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

DS5.9 Prevención, detección y corrección de software malicioso Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

DS5.10 Seguridad de la red Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos sensitivos Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

5.1.2 DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO[2]

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

Control sobre el proceso TI de Administración del ambiente físico que satisface el requisito de negocio de TI para proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio. Enfocándose en proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo. se logra • Implementando medidas de seguridad físicas. • Seleccionando y administrando las instalaciones. y se mide con •

[2] COBIT. IT GOVERNANCE INSTITUTE. CUARTA EDICION, 2007. Pág. 145

Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico • Número de incidentes ocasionados por fallas o brechas de seguridad física • Frecuencia de revisión y evaluación de riesgos físicos.

Objetivos de control detallados

DS12.1 Selección y diseño del centro de datos Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

DS12.2 Medidas de seguridad física Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

DS12.3 Acceso Físico Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

DS12.4 Protección contra factores ambientales Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

DS12.5 Administración de instalaciones físicas Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

5.2 MARCO CONCEPTUAL

Confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.

Disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

Integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

Información es el activo más importante que tienecualquier tipo de organización, ya sea pública o privada, pyme o gran corporación.

Seguridad de la información: tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.La Seguridad de la Información se refiere a la *Confidencialidad, Integridad y Disponibilidad* de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para

detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

La información entonces podría ser clasificada como:

Critica: Es indispensable para la operación de la empresa.

Valiosa: Es un activo de la empresa y muy valioso.

Sensitiva: Debe de ser conocida por las personas autorizadas

ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). la mayoría de estas normas se encuentran en preparación e incluyen:

- ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.
- ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.

- ISO/IEC 27002 - *Information technology - Security techniques - Code of practice for information security management*. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información.

Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 01 de julio de 2007.

- ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 01 de febrero del 2010, No está certificada actualmente.
- ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo

y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

- ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.
- ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. * ISO/IEC 27007 - Es una guía para auditar al SGSI. Se encuentra en preparación.
- ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

COBIT

Es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control ObjectivesforInformationSystems and relatedTechnology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (InformationSystemsAudit and Control Association).[3]

Imagen 1. Modelo COBIT

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

[3] Universidad EAFIT. (10 de Mayo de 2007). *www.eafit.edu.co.* De http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

- Planificación y organización
- Adquisición e implantación
- Soporte y Servicios
- Monitoreo

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Asimismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

6. DISEÑO METODOLOGICO

6.1 TIPO DE ESTUDIO

El tipo de estudio que se llevará a cabo es experimental.En este tipo de estudio el investigador desea comprobar los efectos de una intervención específica, en este caso el investigador tiene un papel activo, pues lleva a cabo una intervención.

En los estudios experimentales el investigador manipula las condiciones de la investigación. En salud se realiza este tipo de estudio, para evaluar la eficacia de diferentes terapias, de actividades preventivas o para la evaluación de actividades de planificación y programación sanitarias.

6.2 METODO DE ESTUDIO

El método de estudio que se llevará a cabo es por observación.

6.3 TECNICAS DE RECOLECCION DE INFORMACION

Se utilizaron técnicas de recolección de información tanto primaria como secundaria. Entre ellas entrevistas con las directivas y docentes de la institución, fotos, videos, listas de chequeos, observación de las instalaciones, observación de libros y documentos importantes como lo es el PEI de la institución.

6.4 INSTRUMENTOS DE RECOLECCION DE INFORMACION

Instrumento: encuesta realizada a estudiantes y docentes del Instituto Reina de los Ángeles.

Propósito: verificar las falencias que presenta la institución que son reconocidas tanto por los directivos como los estudiantes.

6.4.1 DESARROLLO DE ENCUESTA APLICADA A ESTUDIANTES

Se le efectuó la encuesta a un grupo de estudiantes de decimo y undécimo grado de la institución para lograr ver las falencias con las que conviven las personas que habitualmente permanecen en la institución.

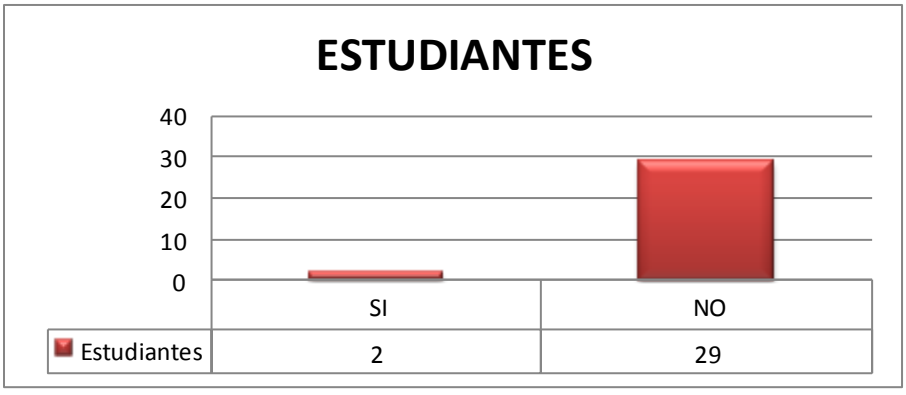
Evaluación de equipos de sala de cómputo

1. ¿El lugar donde se ubica la sala de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?

Grafica 1. SEGURIDAD EN LA SALA DE CÓMPUTO

El 80 % de los encuestados consideran que los equipos de cómputo están seguros de cualquier situación que pueda poner en peligro los equipos de cómputo mientras el otro 20 % no lo considera de esta forma.

2. ¿El lugar donde se ubican los equipos de la sala de cómputo contiene material que pueda ser inflamable o que puedan causar daño a los equipos?



Grafica 2. MATERIAL INFLAMABLE EN LA SALA DE CÓMPUTO

El 93,55 % de los estudiantes encuestados reflejan que las salas de cómputo no contienen algún tipo de material inflamable que pueda causar daño alguno para los equipos de cómputo.

3. ¿La temperatura en que trabajan los equipos de la sala de cómputo es la adecuada para su funcionamiento correcto?

Grafica 3. TEMPERATURA EN LA SALA DE CÓMPUTO

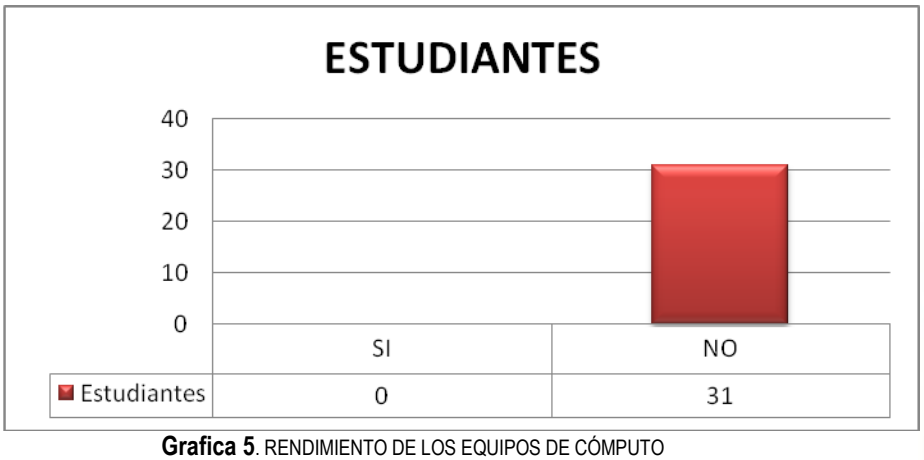
El 87,09 % de los estudiantes encuestados consideran que la sala de cómputo posee una temperatura adecuada que permite el óptimo funcionamiento de los equipos que allí se encuentran.

4. ¿El cableado de la sala de cómputo se encuentra correctamente instalado?

Grafica 4. ESTADO DEL CABLEADO DE LA SALA DE COMPUTO

El 83,8% de los estudiantes que se sometieron a realizar la encuesta respondieron que el cableado de la sala de computo esta correctamente instalado.

5. ¿Los equipos de la sala de cómputo tienen un óptimo rendimiento?



Grafica 5. RENDIMIENTO DE LOS EQUIPOS DE CÓMPUTO

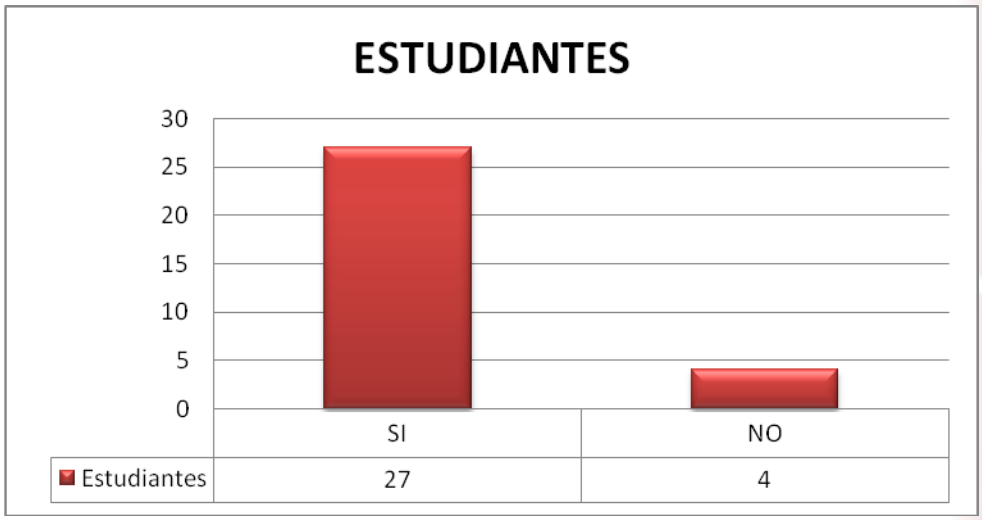
Los equipos de la sala de cómputo tienen un rendimiento inadecuado para los estudiantes que los utilizan, en la encuesta realizada se refleja que el 100% de los estudiantes no están conformes con el desempeño de estos.

6. ¿En la sala de cómputo se le brinda la atención necesaria cuando la requiere?

Grafica 6. ATENCIÓN AL USUARIO EN SALAS DE CÓMPUTO

El 51% de los estudiantes consideran que en las salas de cómputo de la institución la atención que se brinda de manera oportuna, mientras que el 41% de los estudiantes considera que esta información es poco oportuna.

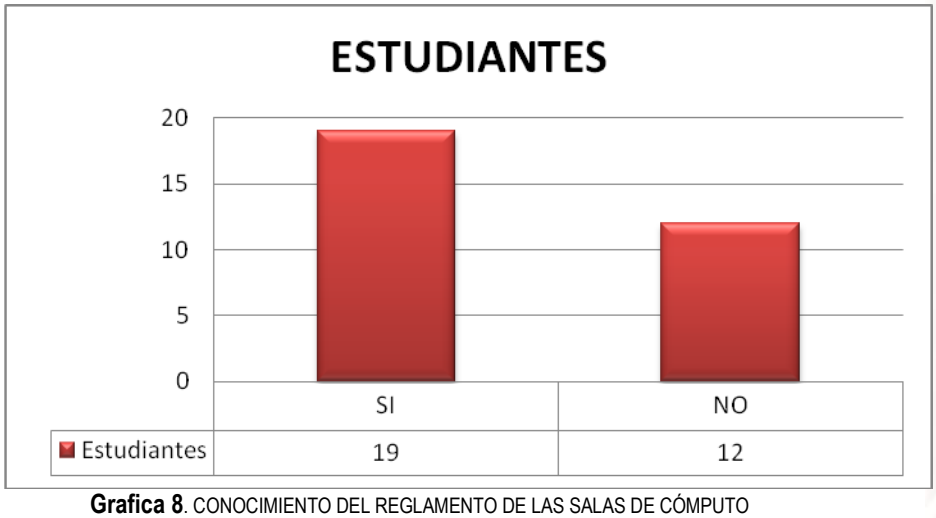
7. ¿Respeta el acceso a la sala de cómputo?



Grafica 7. ACCESO A LA SALA DE CÓMPUTO

El 87% de los estudiantes respetan el acceso a la sala de cómputo, mientras que el 13% refleja que no se respeta el acceso a dicha sala.

8. ¿Conoce el reglamento implementado dentro de la sala de cómputo?

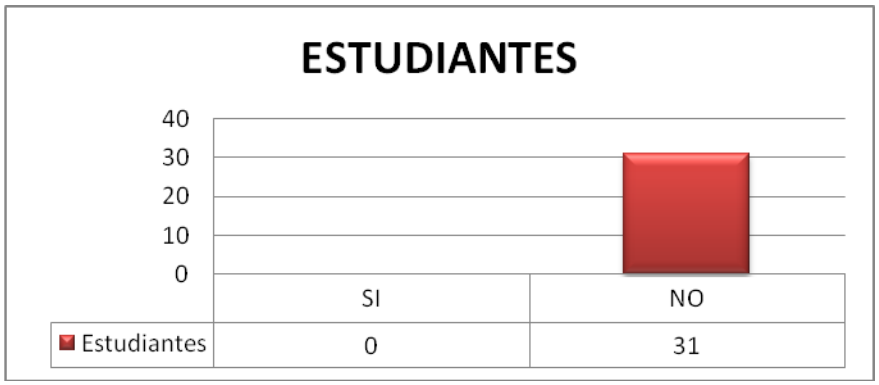


Grafica 8. CONOCIMIENTO DEL REGLAMENTO DE LAS SALAS DE CÓMPUTO

El 61,2% de los estudiantes manifiestan conocer el reglamento implementado dentro de la sala de cómputo según la información revelada por las encuestas mientras que el 38,8% de los estudiantes manifiestan que no conocen este reglamento.

Evaluación de seguridad en la planta física.

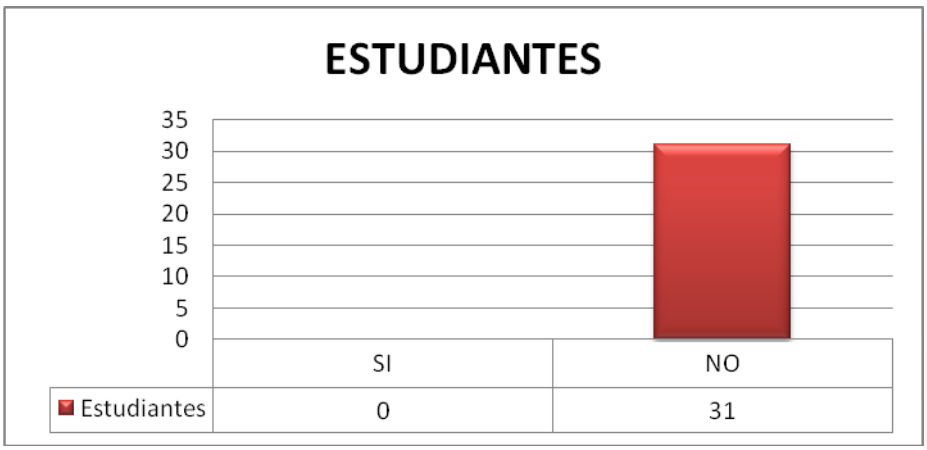
9. ¿Se cuenta con alarma contra incendios?



Grafica 9. UTILIZACION DE ALARMAS CONTRA INCENDIOS

Observamos que el 100% de los estudiantes notan la ausencia de que el instituto reina de los ángeles no cuenta con alarma en caso de incendios.

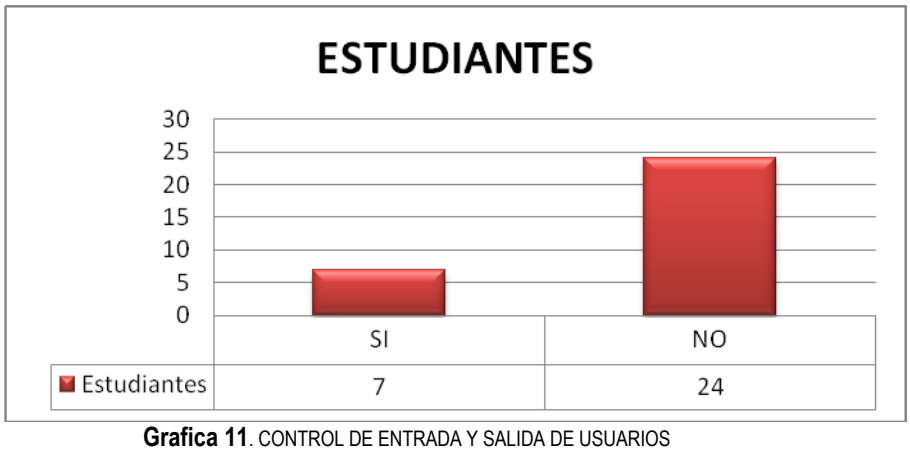
10. ¿Existen extintores?



Grafica 10. UTILIZACION DE EXTINTORES

El 100% de los estudiantes encuestados manifiestan la ausencia de extintores en la institución.

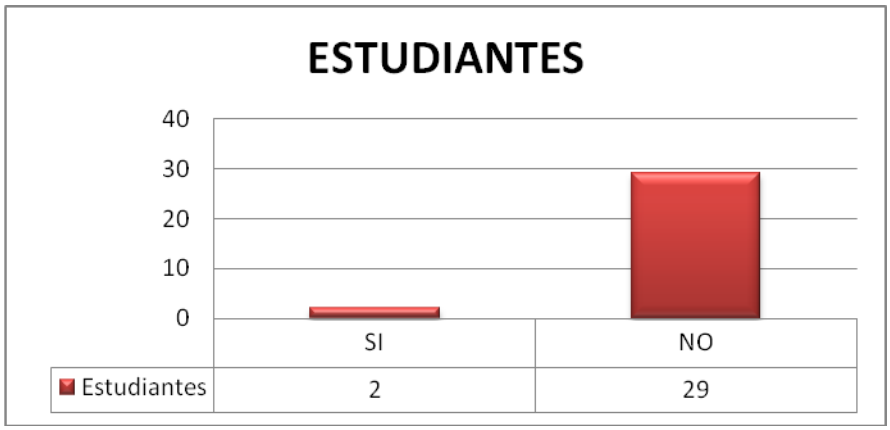
11. ¿Cuentan con algún tipo de control de entradas y salidas de usuarios?



Grafica 11. CONTROL DE ENTRADA Y SALIDA DE USUARIOS

22,5% de los estudiantes encuestados confirman la existencia de control de entrada y salidas de los usuarios al colegio, mientras que el 77,5% manifiestan la ausencia en este control.

12. ¿Existen salidas de emergencia en la institución?



Grafica 12. SALIDAS DE EMERGENCIA

93,5% de estudiantes demuestran que la institución no cuenta con salidas de emergencia o desconocen la existencia de estas, mientras que el 6,5% manifiestan que si se cuenta con salida de emergencia.

6.5 POBLACION DE ESTUDIO

La población de estudio para este proyecto es el Instituto Reina de los Ángeles, institución del departamento del atlántico situada en la ciudad de Barranquilla.

6.6 MUESTRA

Se tomo como muestra 31 estudiantes de los grados de 10 y 11 Instituto Reina de los Ángeles.

7. PLAN DE TRABAJO

Este trabajo de grado permite al **INSTITUTO REINA DE LOS ÁNGELES**, identificar y tomar conciencia de las distintas falencias que presentan hoy día en cuanto a su plataforma tecnológica, seguridad de la información critica, por ello en el desarrollo del trabajo de grado se utilizan diferentes estándares que se consideran como las mejores prácticas para tales fines.

Primero que todo de parte de la institución se realizara una ambientación acerca de cómo funciona la escuela para poder establecer cuáles son los procesos que allí se desarrollan. Luego de entrevistar a los directivos quienes expresaron las inquietudes y preocupaciones que ellos tenían respectos a las falencias constantes que se vienen presentando en la infraestructura tecnológica y seguridad de la información

Después de haber identificado los riesgos y falencias que la institución presenta, el grupo de auditores se encargó de detectar los puntos de mayor criticidad que presenta la institución con el fin de darles las recomendaciones respectivas y de ésta manera reducir el impacto de las amenaza, reduciendo así el costo en que incurriría la institución en el momento en que dichas amenazas se materialicen. Esto lo logramos tomando como punto de referencia el estándar COBIT 4.1 y el estándar ISO 27002.

Para finalizar el trabajo realizado los auditores presentaran un informe final a la institución con el fin de que ellos tomen conciencia de las fallas que presentan y a través de estas recomendaciones tomar las respectivas medidas para mejorar los procesos en los que actualmente están fallando y poder estar a la vanguardia de las diferentes entidades en las que los estándares de auditoría como COBIT e ISO 27002 son de vital importancia debido a que representan mayor seguridad y mejor calidad en la prestación de servicio hacia el cliente final.

8. GESTIÓN DE CONSULTORÍA INTEGRAL"INSTITUTO REINA DE LOS ÁNGELES"

El instituto reina de los ángeles centro de formación de jóvenes preparados para enfrentar los diversos retos de la sociedad, en la búsqueda de estar a la vanguardia de las diferentes entidades que se han dado cuenta de considerar estándares internacionales con el fin de mejorar su funcionamiento interno de esta manera logrando promover su eficiencia y eficacia ante las diferentes entidades que viven del mismo sector económico.

Contacto a nuestro grupo de auditores con el fin de que les ayudáramos con esa tarea que se habían trazado en mejorar, con base a los estándares internacionales existentes para así lograr sobresalir.

Tras una reunión establecida por el grupo de auditores se decidió la implementación o alineamiento con algunos objetivos de control que contiene COBIT estándar internacional aceptado y acogido por muchas entidades con gran reconocimiento.

8.1 RECONOCIMIENTO DE INSTALACIONES Y NECESIDADES DE LA INSTITUCION

Inicialmente tras una conversación por parte del grupo de auditoría y los directivos de la institución se logro definir los puntos sobre los que había que trabajar fuertemente.

Imagen 2. Fachada de la institución

El reconocimiento de las instalaciones de la institución es de vital importancia debido a que este da una idea sobre el ambiente tecnológico y social manejado en la institución, las necesidades planteadas por los directivos fueron muchas de las cuales solo a través de este trabajo de grado cubrir algunas.

Imagen 3. Sala de cómputo

Imagen 4. Sala de cómputo

8.2 ENTREGA DE PROPUESTA DE AUDITORIA

Luego de haber realizado la respectiva identificación de los puntos a tratar y de los riegos a corregir el equipo planteo una propuesta de auditoría donde se plasmaba el compromiso por parte del equipo hacia el instituto reina de los ángeles.

A continuación se muestra la propuesta entregada por de auditores:

INSTITUTO REINA DE LOS ANGELES

Barranquilla, 10 de mayo de 2010

Señora

Noemí Joleani

Directora

REF: Auditoria Integral Instituto Reina de los Ángeles.

De acuerdo al plan de auditoría, damos inicio a la auditoría en referencia, en el período de tiempo comprendido del 10 de mayo al 30 de septiembre del presente año; la cual será desarrollada por los auditores:

Julieth Córdoba
María Angélica Martí
Fabio Mendoza

A continuación describimos los objetivos y el alcance de ésta auditoría:

Objetivos.

- Identificar controles existentes enfocados a la seguridad del instituto (Plataforma TI).
- Identificar la información confidencial de la institución.
- Verificar la seguridad en las aplicaciones (métodos de control acceso).
- Generar lineamientos que permitan soportar y mitigar en gran manera las brechas de seguridad física y de la información que se presentan en la actualidad en el instituto.

Alcance

Para la realización de la siguiente auditoría se tuvo en cuenta los siguientes aspectos:

- Análisis de riesgos en la plataforma tecnológica de la institución.
- Evaluación de permisos y roles de los directivos de la institución.
- Evaluación del proceso utilizado para el paso de notas al sistema.
- Verificación de existencia de manuales de usuarios, funciones y técnicos dentro de la institución.

Teniendo en cuenta los objetivos y alcance mencionados en la auditoría el cronograma es susceptible a modificaciones.

Agradezco de antemano su colaboración,

Cordialmente,

_____

Julieth Córdoba Díaz
Auditora de Sistemas y Seguridad.
CC. 1129509113 B/quilla

_____

María Angélica Martí Porto
Auditora de Sistemas y Seguridad.
CC. 1129583466 B/quilla

_____

Fabio Mendoza
Auditor de Sistemas y Seguridad.
CC. 1045667290 B/quilla

8.3 CREACIÓN DE PLAN DE CRONOGRAMA DE ACTIVIDADES

Inmediatamente de haber realizado lo concerniente a la identificación de los puntos a tratar y de los riegos a corregir el equipo planteo un cronograma de actividades donde se realizo la planeación completa de los pasos a seguir para lograr conseguir minimizar las falencias y riesgos que la institución presentaba desde un inicio.

Este cronograma fue realizado con base al conocimiento adquirido durante la formación obtenida en la especialización.

Para la realización del cronograma se tuvo en cuenta los rangos de horas en los cuales los directivos de la institución nos podían atender debido a que por su rol que manejan dentro de la escuela tienen una carga ocupacional muy elevada.

ACTIVIDADES	Horas	MESES																					
		MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE			
		Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4
PRESENTACION DE AUDITORIA	2																				
CONOCIMIENTO DE LA INSTITUCIÓN	12																				
ENTREGA PROPUESTA DE AUDITORIA	2																				
IDENTIFICACIÓN DE RIESGOS	48																				
ANALISIS DE RIESGOS	48																				
IDENTIFICACIÓN DE CONTROLES EXISTENTES	24																				
EVALUAR CONTROLES EXISTENTES	24																				
IDENTIFICAR Y PROPONER OPCIONES DE TRATAMIENTO	72																				
PREPARACION INFORME AUDITORIA	24																				
ENTREGA INFORME FINAL DE AUDITORIA	2																				

Imagen 5. Cronograma de Actividades

8.4 IDENTIFICACIÓN DE RIESGOS

Riesgo: "Es el costo o valor de las pérdidas que sufre o se expone a sufrir una organización, como consecuencia de las manifestaciones de situaciones no deseadas denominadas causas o amenazas de riesgo y efectos." Considerando lo perjudicial que puede ser para la institución reina de los

ángeles que se materialice alguno de los riesgos que dicha entidad presenta, nuestro equipo de auditores se encargo de identificar los riesgos de mayor impacto, utilizando los diferentes métodos aprendidos durante la formación de la especialización y dejando evidencias inmediatas que reflejan la veracidad y existencia de las fallas encontradas.

A continuación se muestran los riesgos de la plataforma física de la institución con sus respectivas evidencias y recomendaciones para su solución.

8.4.1 SEGURIDAD DE LOS SISTEMAS

- Ingreso no percibido al sistema por inexistencia de cuentas de usuario.

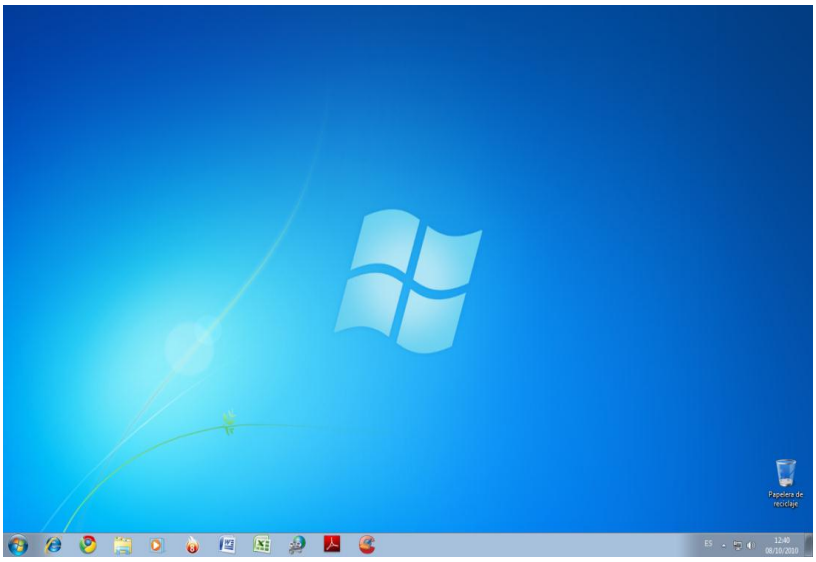


Imagen 6. Ingreso no percibido al sistema

Con esta falencia encontrada en el equipo de cómputo **servidor** se está violando los siguientes objetivos de control que se encuentran en ISO 27002 y COBIT cuyos nombres son:

Objetivos de Control ISO 27002	Objetivos de Control COBIT
11.5 Control de Acceso al sistema Operativo	**DS5. Garantizar la seguridad de los sistemas**

11.5.1 Procedimientos de inicio seguro	DS5.4 Administración de cuentas de usuario.

- Manipulación de la información confidencial de la institución por parte de terceros por falta de seguridad en los archivos y carpetas.

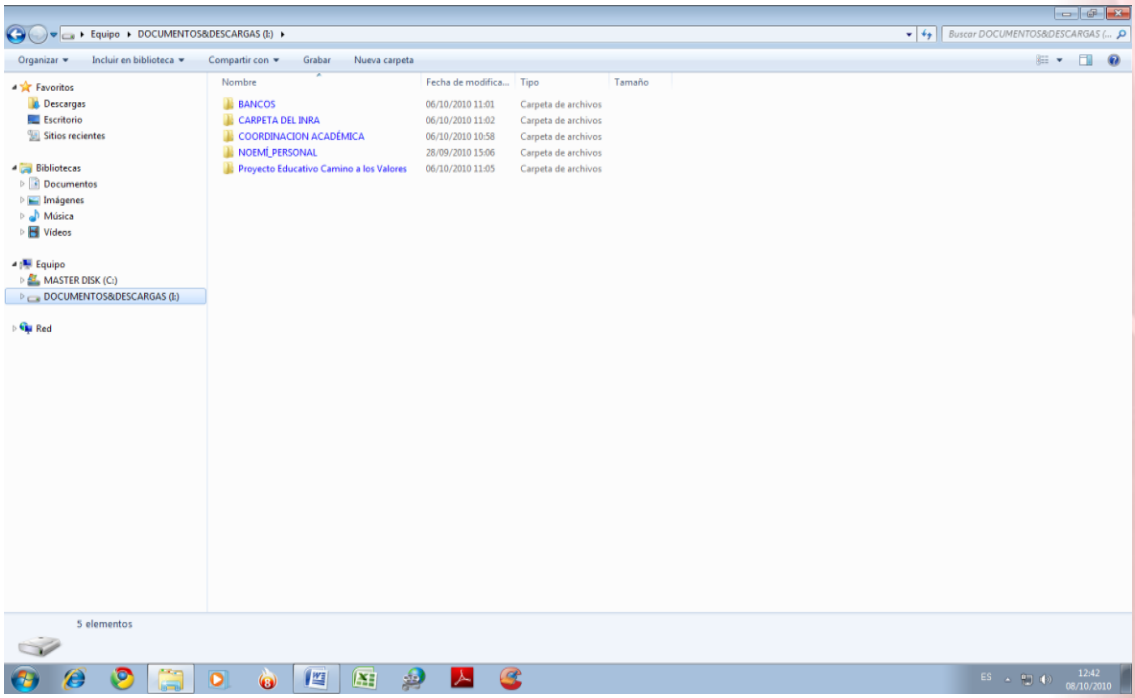


Imagen 7. Manipulación Carpetas Contenedoras de Información.

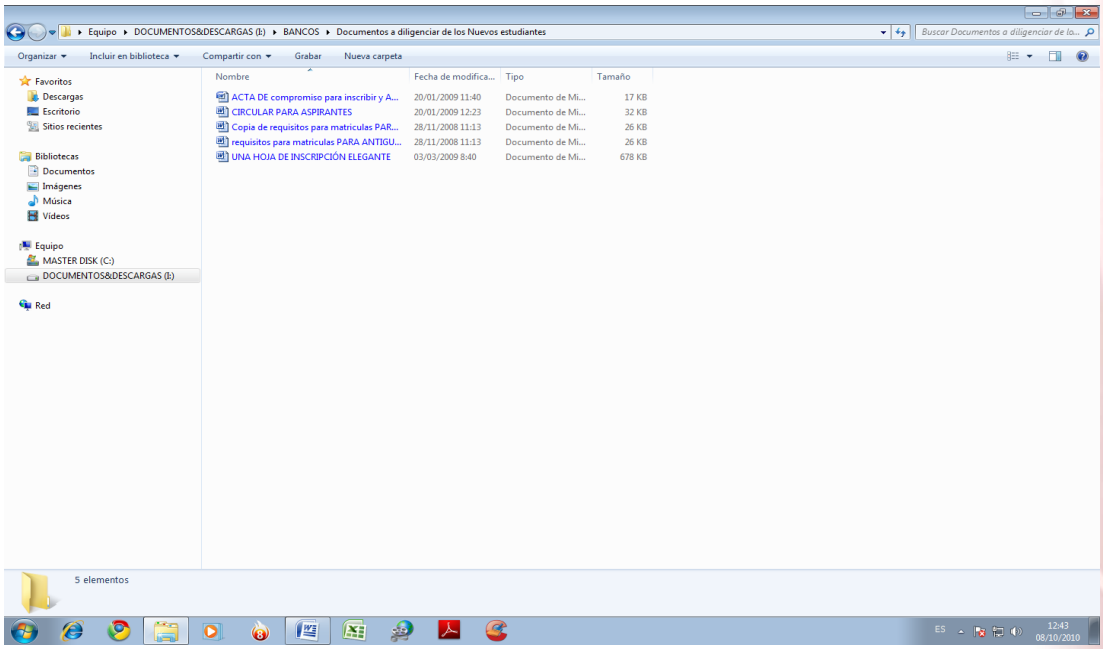


Imagen 8. Manipulación de Archivos.

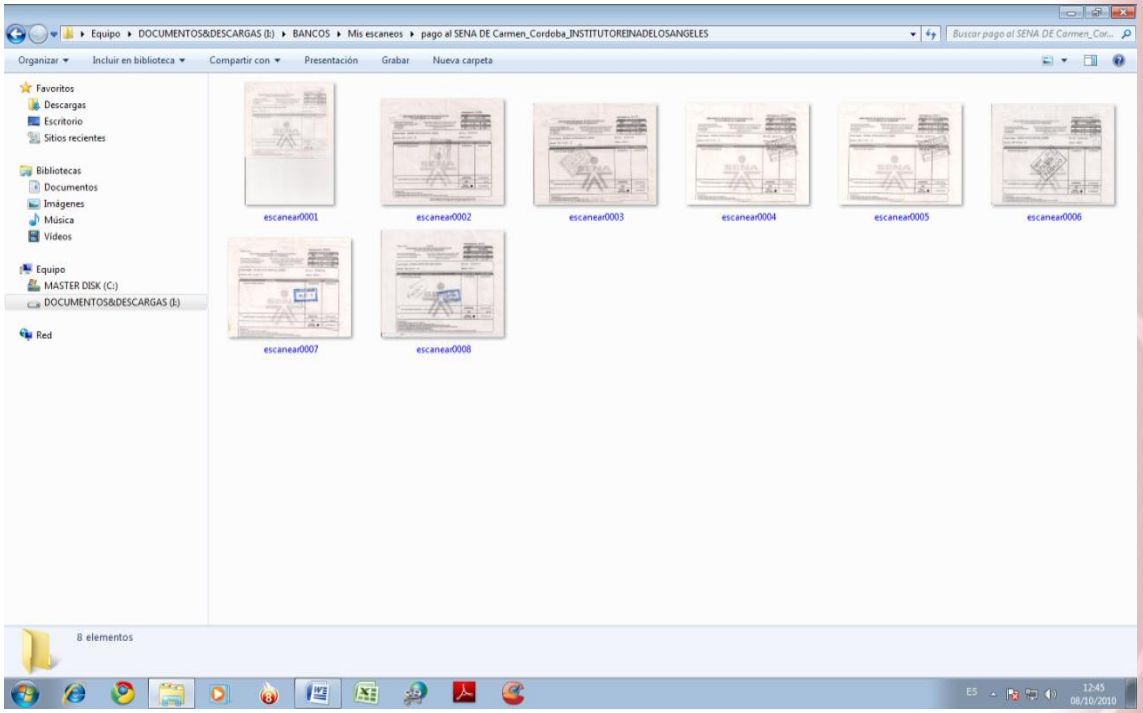


Imagen 9. Manipulación de Archivos de pago

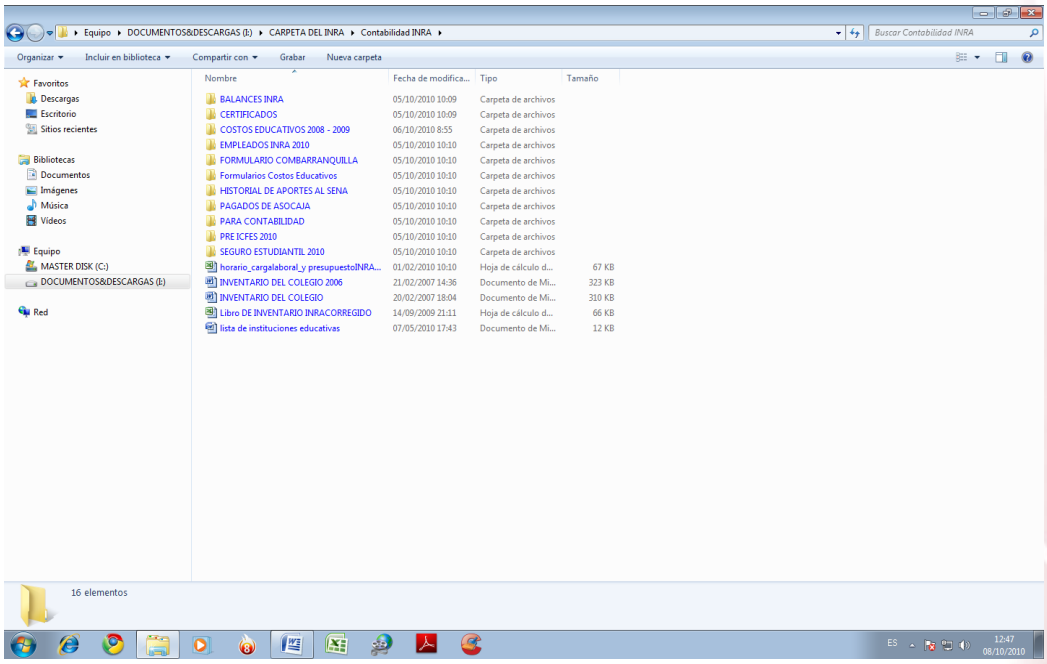


Imagen 10. Manipulación de Información.

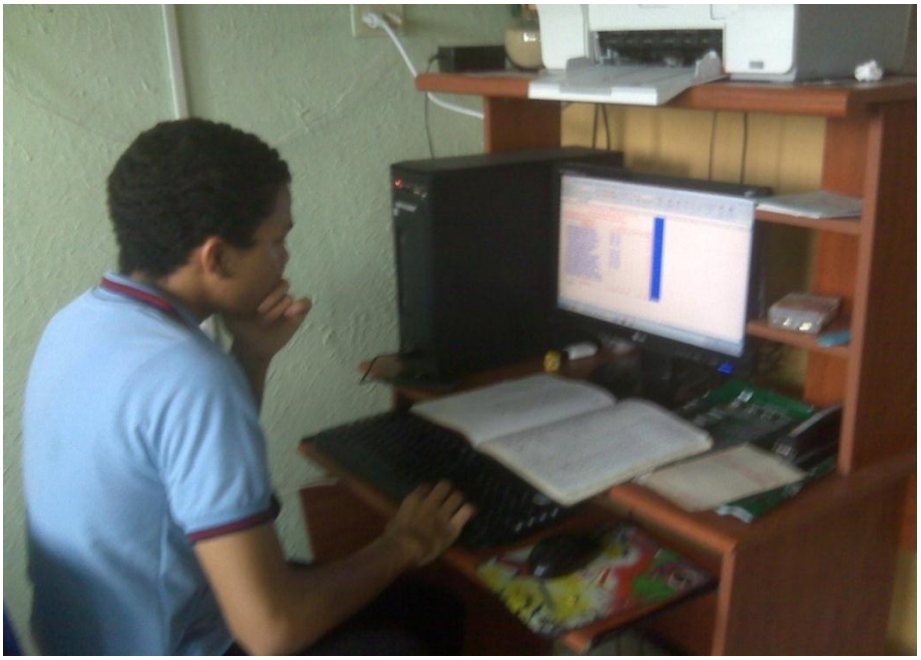


Imagen 11. Manipulación de archivos de notas

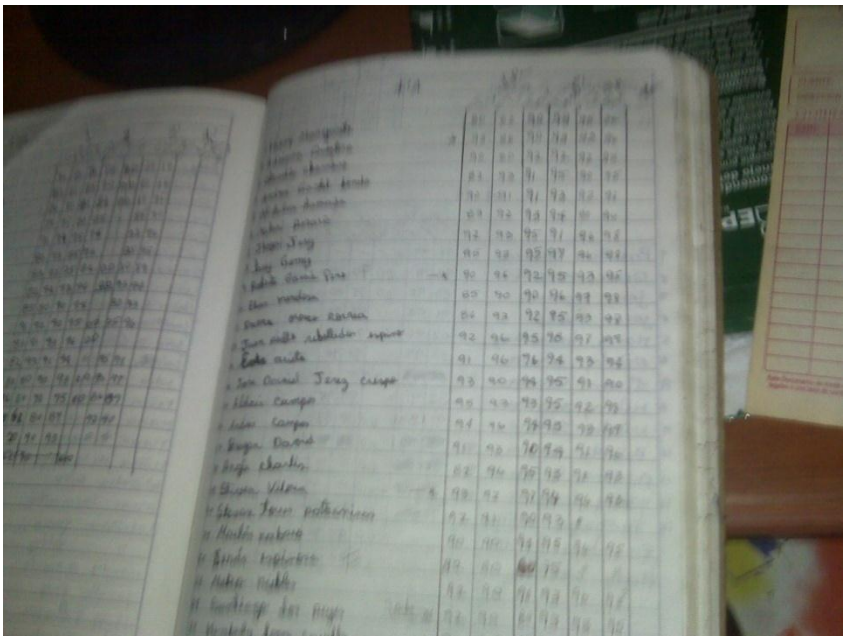


Imagen 12. Ausencia de Control de Acceso a Información Relevante

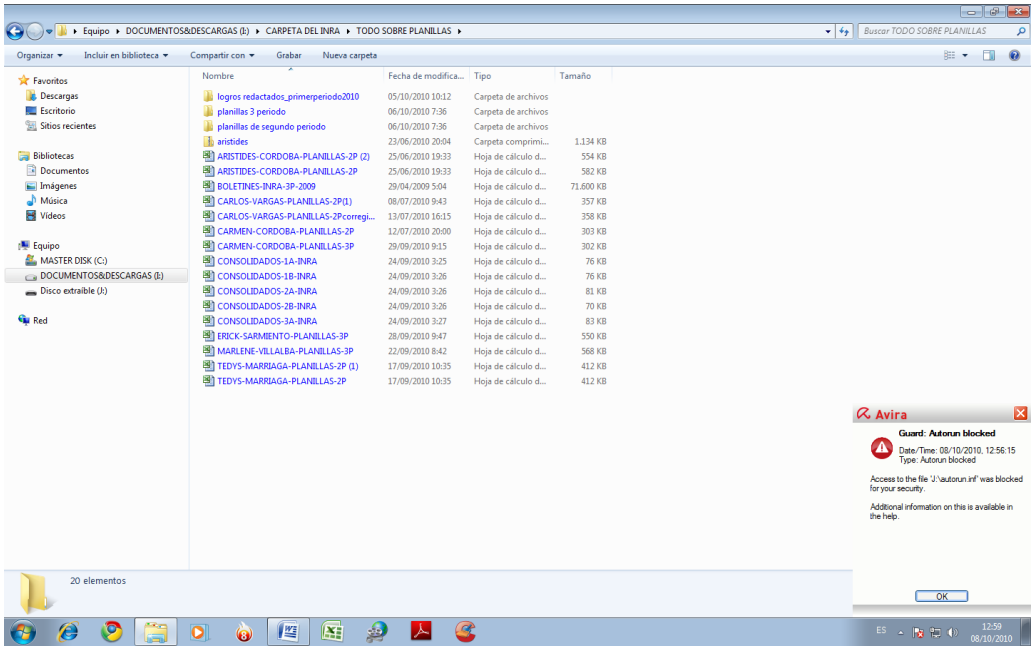


Imagen 13. Ausencia de actualizaciones de antivirus

Con esta falencia encontrada se está violando los siguientes objetivos de control que se encuentran en ISO 27002 y COBIT cuyos nombres son:

Objetivos de Control ISO 27002	Objetivos de Control COBIT
11.5 Control de Acceso al sistema Operativo	**DS5. Garantizar la seguridad de los sistemas**
11.6 Control de acceso a las aplicaciones y a la información	**DS5.4 Administración de cuentas de usuario.**
11.6.1 Restricción de acceso a la información	
11.7 Computación móvil y trabajo remoto	

8.4.2 ADMINISTRACIÓN DEL AMBIENTE FÍSICO

- Pérdida de material de trabajo por falta de controles de acceso al permitir el ingreso de personal no autorizado a las diferentes oficinas donde se encuentran los equipos de cómputo

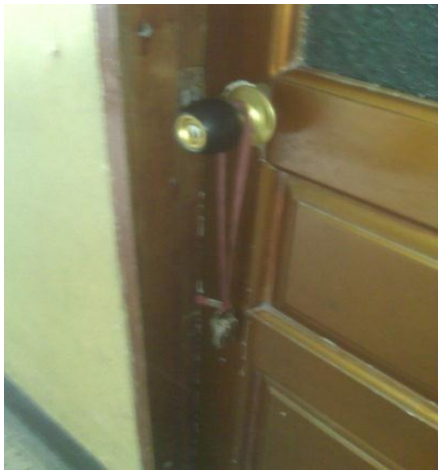


Imagen 14. Ausencia de Control de Ingreso a Oficinas

- Violación de confidencialidad por copia de la información, mediante el acceso sin restricción de personal del plantel al lugar donde se encuentra los back-up de información.

Imagen 15. Almacenamiento de Back-up

Imagen 16. Lugar donde almacenan Archivos Confidenciales

Con esta falencia encontrada se está violando los siguientes objetivos de control que se encuentran en ISO 27002 y COBIT cuyos nombres son:

Objetivos de Control ISO 27002	Objetivos de Control COBIT
9.Seguridad física y del entorno	**DS12.3 Acceso Físico**
9.1 Áreas seguras	
9.1.1 Perímetro de seguridad Física	
9.1.2 Controles de acceso físico	

9.1.3 Seguridad de oficinas, recintos e instalaciones	
9.2 Seguridad de los equipos	

- Ausencia de aire acondicionado para controlar la temperatura del lugar donde funciona el servidor.

Imagen 17. Oficina donde se encuentra el Servidor

Imagen 18. Instalaciones eléctricas de sala de cómputo.

Imagen 19. Aire acondicionado de sala de cómputo

Objetivos de Control ISO 27002	Objetivos de Control COBIT
9.1.4 Protección contra amenazas externas y ambientales.	DS 12.4
9.2.1 Ubicación y protección de los equipos	DS 12.5
9.2.3 Seguridad del cableado.	

9. ENTREGA DE INFORME FINAL DE AUDITORIA

Barranquilla, Septiembre 27 de 2010

Señora
Noemí Joleani
Directora Instituto Reina de los Ángeles
E. S. M.

Ref: Informe con los resultados de la Auditoría al instituto reina de los ángeles, Infraestructura Física, tecnológica.

Cordial saludo,

Nos complace presentar a su consideración el informe con los resultados de la Auditoría efectuada.

1. OBJETIVOS Y ALCANCE DE LA AUDITORIA

La auditoría tuvo como objeto:

- Identificar los riesgos en las instalaciones en donde se encuentren equipos de cómputo y servidores (existencia de salidas de emergencia, extintores, zonas seguras, planes de evacuación, entre otros).
- Identificar controles existentes enfocados a la seguridad del instituto (Física y de sistemas).
- Verificar la seguridad en las aplicaciones (métodos de control acceso).
- Generar lineamientos que permitan soportar y mitigar en gran manera las brechas de seguridad física y de la información que se presentan en la actualidad en el instituto.

La auditoría enfatizó en los controles necesarios para minimizar la probabilidad de ocurrencia de los cuatro (4) riesgos potenciales resultantes como críticos en el Análisis de Riesgos efectuado: Estado de infraestructura física en donde se encuentran equipos de cómputo, de la infraestructura tecnológica y de la seguridad de la información confidencial.

2. METODOLOGIA EMPLEADA

La Auditoría se desarrolló de acuerdo con las normas de auditoría generalmente aceptadas, especialmente las promulgadas para la Auditoría de Sistemas de Información por ISACA (InformationSystemsAudit and Control Association, Inc).

Para satisfacer los objetivos de la auditoría se desarrollaron los siguientes pasos y procedimientos:

a. Se efectuaron entrevistas con la funcionaria Noemí Joleani, encargada de la dirección del instituto.

b. Con base en las falencias que evidenciamos se inició el proceso de auditoría enfatizando en los riesgos críticos encontrados. Este proceso consistió en a) Identificar las causas de los riesgos críticos. b) Identificar y evaluar los controles utilizados. c) Diseñar y ejecutar las pruebas de auditoría en los diferentes equipos de cómputo y d) Elaboración y presentación del informe con los resultados de la Auditoría.

3. RESULTADOS DE LA AUDITORIA

3.1. OPINION DE LA AUDITORIA

- En nivel de riesgo por plagio y/o pérdida de información es alto debido a que no se tiene control restrictivo para el uso de la cuenta de administrador, ni la definición de cuentas de usuario, como tampoco al acceso de documentos físicos con información confidencial (notas, hojas de vida de estudiantes, etc)
- Las instalaciones donde funcionan los salones de cómputo no poseen las condiciones ambientales, locativas y de seguridad requeridas.

3.2. PRINCIPALES RECOMENDACIONES Y PUNTOS MEJORABLES

Garantizar la seguridad de los sistemas

- La dirección debe aprobar un documento de política de seguridad de la información, publicarlo y comunicarlo a todos los empleados. El documento debe tener estipulado la

creación de cuentas de usuario con sus respectivos permisos para impedir el acceso a personal no autorizado y permisos adecuados para su cargo.

- Definir claramente las responsabilidades en cuanto a la seguridad de la información.
- Identificar, documentar e implementar las reglas sobre el uso aceptable de la información.
- La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
- Todos los empleados de la institución deberían recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización según sea pertinente para sus funciones laborales.
- Debería existir un proceso disciplinario formal para los que comentan alguna violación de seguridad.
- Establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar en donde se encuentra el servidor. Este que maneja datos sensibles, debería estar ubicados de tal forma que se reduzca el riesgo de visualización de la información por personas no autorizadas durante su uso y los sitios de almacenamiento se deberían asegurar para evitar el acceso no autorizado.
- Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
- Restringir la descarga inescrupulosa de programas y su instalación, solo permitir que personal autorizado lo haga.
- Hacer una política de respaldo de la información, para copias de seguridad de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
- Se debería registrar la fecha y hora de entrada y salida de usuarios tanto a las instalaciones de las salas de cómputo como al equipo servidor que contiene la información confidencial de la institución.
- Se deberían establecer directrices para no permitir comer, beber, fumar dentro centro de cómputo y en las instalaciones donde se encuentra el servidor encargado del almacenamiento de información.

- Establecer una política formal que prohíba el uso de software no autorizado y procedimientos para el manejo de la información con el fin de protegerla contra divulgación o uso sin permiso adecuado.
- Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.
- La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.
- Todos los usuarios deberían tener un identificador único (ID del usuario) para su personal, y se debería elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.
- La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.
- Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

Administración del ambiente físico

- Definir o diseñar un esquema del centro de datos teniendo en cuenta los riesgos asociados con desastres naturales y causados por el hombre.
- Debe considerar las leyes y regulaciones tales como regulaciones de seguridad y de salud de trabajo.
- Deben instalarse dispositivos y equipos especializados de acuerdo a las necesidades del negocio para monitorear y controlar el ambiente.
- Las instalaciones claves se deberían ubicar de modo que se evite el acceso al público.
- La adquisición de un aire acondicionado para el lugar donde se encuentra el servidor, previene el daño en el equipo a causa del recalentamiento ocasionado por las altas temperaturas presentadas en dicho lugar.
- El uso de reguladores en los equipos de la sala de cómputo y del servidor ayudan a proteger de las diferencias de voltaje que se pueden presentar en las instalaciones eléctricas de la institución.

Se hace entrega de este informe el día 28 de Septiembre de 2010 a los señores Noemí Joleani

Cordialmente,

_____

Julieth Córdoba Díaz
Auditora de Sistemas y Seguridad.
CC. 1129509113 B/quilla

_____

María Angélica Martí Porto
Auditora de Sistemas y Seguridad.
CC. 1129583466 B/quilla

_____

Fabio Mendoza
Auditor de Sistemas y Seguridad.
CC. 1045667290 B/quilla

CONCLUSIONES

Estar en búsqueda de un constante nivel educativo motivó al Instituto Reina de los ángeles a considerar la auditoria de sistemas como una herramienta que le permita fortalecer de manera eficaz muchos de sus procesos, esta evaluación soportada en los más importantes estándares de calidad le brindaron a la institución una visión más amplia de cómo llevar la seguridad física de sus instalaciones, la seguridad de su información y de sus sistemas a un estado mucho más óptimo.

Por este motivo, fortalecer factores considerados claves para el desempeño de la institución fue parte prioritaria en la realización de esta auditoría.

Buscar proteger las herramientas y aplicaciones informáticas con las que se cuenta, enseñándoles a hacer una clasificación óptima de su información fue uno de los objetivos logrados en el desarrollo de esta tesis, además mostrándoles la importancia de mantener un ambiente físico óptimo que fuese acorde con las necesidades del negocio para así lograr mantener sus activos en cuanto a infraestructura tecnológica y de la información se refiere.

Estas fueron las bases que permitieron que este proyecto se convirtiese en una realidad y a su vez en una ventaja competitiva para la institución educativa.

ISO 27002 y Cobit 4.1 fueron los marcos de trabajo en los que nos basamos para sustentar todos los cambios y recomendaciones que buscamos generar en la institución y que se implementarán en la medida en que los directivos del **INRA** lo consideren oportuno.

Este proyecto buscó dejar un precedente en el Instituto Reina de los Ángeles, un lineamiento que le permita conocer las mejores prácticas del mercado para soportar la seguridad de su información y la administración de su ambiente físico.

Sabemos que a través del desarrollo de este trabajo hemos logrado brindar a la institución educativa una mejor imagen frente a sus stakeholders a través de la generación de valor dada al aplicar los controles sugeridos y al lograr la identificación oportuna de sus principales riesgos.

BIBLIOGRAFIA

- Proyecto de norma tecnica colombiana NTC-ISO/ IEC 27002.
- IT governance institute.Cobit 4.1
- www.isaca.org

ANEXOS

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01
		FECHA: Febrero 2011
		CODIGO:DOC-VACRE-NETGUDI

ANEXO 1
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Barranquilla, Fecha

Marque con una X
Tesis ☐ **Trabajo de Grado** ☐

Yo Julieth Katerine Cordoba Diaz, identificado con C.C. No. 1129509113, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado Auditoria Integral al Instituto Reina de los Angeles presentado y aprobado en el año 2011 como requisito para optar al título de Especialista en Auditoria a los sistemas de información hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los ____días del mes de Abril de Dos Mil Once 2011

EL AUTOR - ESTUDIANTE. Julieth Cordoba

FIRMA

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01
		FECHA: Febrero 2011
		CODIGO:DOC-VACRE-NETGUDI

ANEXO 1
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Barranquilla, Fecha

Marque con una X
Tesis ☐ **Trabajo de Grado** ☐

Yo María Angelica Martí Porto, identificado con C.C. No. 1129583466; actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado Auditoria Integral al instituto Reina de los Angeles. presentado y aprobado en el año 2011, como requisito para optar al título de Especialista en auditoria de Sistemas de Información;
hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los ____días del mes de Abril de Dos Mil once 2011

EL AUTOR - ESTUDIANTE. María Angelica Martí P
FIRMA

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01
		FECHA: Febrero 2011
		CODIGO:DOC-VACRE-NETGUDI

ANEXO 1
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Barranquilla, Fecha

Marque con una X
Tesis ☐ **Trabajo de Grado** ☐

Yo Fabio Enrique Mendoza Palechor, identificado con C.C. No. 1045667290, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado Auditoria Integral Instituto Reina de los Angeles presentado y aprobado en el año 2011 como requisito para optar al título de Especialista en Auditoria a los Sistemas de Información; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los ____días del mes de Abril de Dos Mil Once 200 11

EL AUTOR - ESTUDIANTE. Fabio Mendoza Palechor
FIRMA

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01 FECHA: Febrero 2011 CODIGO:DOC-VACRE-NETGUDI

ANEXO 2
F ORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO:

Auditoria Integral Instituto Reina De los Angeles

SUBTÍTULO, SI LO TIENE:

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Cordoba Diaz Marti Porto Mendoza Palechor	Julieth Maria Angelica Fabio Enrique.

DIRECTOR (ES)

Apellidos Completos	Nombres Completos

JURADO (S)

Apellidos Completos	Nombres Completos
Montaño-Ardila	Victor Manuel

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos
Duello Florez	Osvaldo Rafael

TRABAJO PARA OPTAR AL TÍTULO DE: Especialista En Auditoria a los Sistemas

FACULTAD: Pos-Grado

PROGRAMA: Pregrado ____ Especialización X

NOMBRE DEL PROGRAMA Especialización En Auditoria A los Sistemas de Información

Barranquilla, 12 Abril del 2011

Ingeniero:
Victor Montaño Ardila
Coordinador Especialización Auditoria a los Sistemas de Información
Ciudad

El abajo firmante asesor del trabajo de grado titulado:

"AUDITORIA INTEGRAL INSTITUTO REINA DE LOS ÁNGELES".

Certifico que el **PROYECTO DE GRADO** ha sido evaluado, lográndose los alcances establecidos en el proyecto.

Cordialmente.

ASESOR METODOLÓGICO

OSVALDO PUELLO FLOREZ